New York Journal of Mathematics

New York J. Math. **28** (2022) 494–522.

Some braces of cardinality p^4 and related Hopf-Galois extensions

D. Puljić, A. Smoktunowicz and K. Nejabati Zenouz

ABSTRACT. We describe all $\mathbb{F}_p$-braces of cardinality p^4 which are not right nilpotent. The constructed braces are solvable and prime, and contain a non-zero strongly nilpotent ideal. We use the constructed braces to construct examples of finitely dimensional pre-Lie algebras which are left nilpotent but not right nilpotent. We also explain some well known results about the correspondence between braces and Hopf-Galois extensions using the notion of Hopf-Galois extensions associated to a given brace. This can be applied to the constructed $\mathbb{F}_p$-braces.

CONTENTS

1. Introduction

In 2005, W. Rump introduced braces as a generalisation of Jacobson radical rings in order to help study involutive set-theoretic solutions of the Yang-Baxter equation. Since then braces have been studied solely for their algebraic properties and have been linked to other research areas. For example, T. Gateva-Ivanova showed that braces are in correspondence with braided groups with an involutive braiding operator in [10]. Braces have also been shown to be equivalent to some objects in group theory such as bijective 1-cocycles and regular

Received September 15, 2021.
2010 *Mathematics Subject Classification.* 16W35, 16T25, 81R50.
Key words and phrases. Braces, Hopf-Galois extensions.
The second author is supported by the EPSRC grants EP/V008129/1 and EP/R034826/1.

ISSN 1076-9803/2022

subgroups of the holomorph and they have been studied in connection to flat manifolds, quantum integrable systems, etc. Further, skew braces were introduced in [11], as a generalisation of braces, and D. Bachiller followed to discover that there is a connection between skew braces and Hopf-Galois theory which was further studied in [21].

The above evidences the value of classifying braces, which is a direction research has taken in recent years. Braces with cyclic additive groups were classified in [14, 15] and braces of size pq and p^2q for primes p and q were classified in [1] and [9], respectively. All braces of cardinality p^3 have been described by D. Bachiller [2] and all skew braces of the same size by K. Nejabati Zenouz [13]. In [22] L. Vendramin suggested that the problem of classification of braces of order p^n could be tackled by considering $\mathbb{F}$-braces, which is the framework of this paper.

The general aim of our paper is to develop ring theoretic themes in the main calculations of characterising the braces as opposed to more group theoretic themes. Our method of choice is constructing braces using generators and relations. Notice that some other methods of constructing braces, for example by linking two homomorphisms of abelian and multiplicative groups, were considered in [2, 13]. When constructing braces it is often difficult to check if the brace compatibility condition, $a\circ(b+c)+a = a\circ b + a\circ c$, holds, because of the large amount of choices for a, b, c. This problem is particularly pertinent for braces which are not right nilpotent. Indeed, several methods exist for characterising all right nilpotent braces of cardinality p^n, such as an extension by the socle [2], and by using the group of flows of pre-Lie algebras [17, 20]. However, these methods are not available to characterise braces which are not right nilpotent. On the other hand, it was mentioned on page 22 of [22] that braces with additive group C_p^5, for $p = 2, 3$, pose a special difficulty for the GAP package. In this paper we construct all braces of cardinality p^4 which are not right nilpotent and whose additive group is C_p^4. We hope that similar methods could be applied in future to help with GAP calculations for braces of cardinality p^5 and p^6. Problem 2.18 from [22], which asks to compute automorphisms groups of skew left braces of size p^n, could also be related for the special case of $n = 4$. A motivation for aforementioned investigations was mentioned in [2] "for any brace structure that we can determine, we are also computing a solution to the Yang-Baxter equation. Another important thing about braces is their connection with other algebraic structures. For all these reasons, a classification of all finite braces of finite order is wanted."

We also partially answer a question asked in [22], namely the characterisation of all skew braces of cardinality p^n (Problem 2.14, [22]). Our main result is Theorem 6.3, which describes all $\mathbb{F}_p$-braces of cardinality p^4 which are not right nilpotent. Our results hold for $p > 3$ and braces of cardinality p^4 for $p = 2, 3$ can be calculated using the GAP package. Notice that finite $\mathbb{F}_p$-braces are exactly skew braces whose additive group is C_p^n (see the Background Information

section below for more details). We also investigate connections of our results with Hopf-Galois extensions.

2. Background information

Recall that a set A with binary operations $+$ and $*$ is a *left brace* if $(A,+)$ is an abelian group and the following version of distributivity combined with associativity holds:

$$(a+b+a*b)*c = a*c+b*c+a*(b*c), \tag{1}$$
$$a*(b+c) = a*b+a*c$$

for all $a,b,c \in A$. Moreover, $(A,\circ)$ is a group, where we define

$$a\circ b = a+b+a*b.$$

In what follows, we will use the definition in terms of operation '$\circ$' presented in [6] (see [16] for the original definition): a set A with binary operations of addition $+$, and multiplication $\circ$ is a brace if $(A,+)$ is an abelian group, $(A,\circ)$ is a group and for every $a,b,c \in A$

$$a\circ(b+c)+a = a\circ b + a\circ c.$$

Circle algebras related to braces were introduced by Catino and Rizzo in [5]. A special case of circle algebras are radical circle algebras. Notice that radical circle algebras satisfy the definition 2 from [17], and hence radical circle algebras are exactly right $\mathbb{F}$-braces. To obtain the corresponding brace, we change the multiplication to the opposite multiplication in our brace, $a\circ b \to b\circ a$. We now recall definition 2 from [17], which we state for left braces, as it was originally stated for right braces.

Definition 2.1. *Let $\mathbb{F}$ be a field. We say that a left brace A is an $\mathbb{F}$-brace if its additive group is an $\mathbb{F}$-vector space such that $a*(\alpha b) = \alpha(a*b)$ for all $a,b \in A$, $\alpha \in \mathbb{F}$. Here $a*b = a\circ b - a - b$.*

Notice that finite left $\mathbb{F}_p$-braces are exactly braces whose multiplicative group is C_p^n, where C_p is the cyclic group of cardinality p. Indeed, if A is an $\mathbb{F}_p$-brace then it is a vector space over $\mathbb{F}_p$, hence $pa = 0a = (p-p)a = pa - pa = 0_A$ where 0_A is the identity of the additive group $(A,+)$, and pa is the multiplication of $p \in \mathbb{F}_p$ and $a \in A$ in our vector space. Note that $1a = a$ for $1 \in \mathbb{F}_p$ by the definition of a vector space. Therefore, every element in $(A,+)$ has order at most p, and since $(A,+)$ is abelian it follows that $(A,+)$ is C_p^n. On the other hand, let $(A,+,\circ)$ be a brace whose additive group is C_p^n, then we can define $1a = a$ for $1 \in \mathbb{F}_p$ and $a \in A$, and it gives a well defined $\mathbb{F}_p$-brace. Observe that the compatibility relation $b*(ia) = i(b*a)$ holds in this brace for integers i, because $b*(ia) = b*(a+...+a) = a*b+a*b+...+a*b = i(a*b)$ by the brace relation $x*(y+z) = x*y+x*z$. Since $a \neq 0$ has the additive order p, then $pa = a+a+...a = 0$, hence A is an $\mathbb{F}_p$-brace.

In [16], Rump introduced *left nilpotent* and *right nilpotent* braces and radical chains $A^{i+1} = A*A^i$ and $A^{(i+1)} = A^{(i)}*A$ for a left brace A, where $A =$

$A^1 = A^{(1)}$. Recall that a left brace A is left nilpotent if there is a number n such that $A^n = 0$, where inductively A^i consists of sums of elements $a * b$ with $a \in A, b \in A^{i-1}$. A left brace A is right nilpotent if there is a number n such that $A^{(n)} = 0$, where $A^{(i)}$ consists of sums of elements $a * b$ with $a \in A^{(i-1)}, b \in A$. Strongly nilpotent braces and the chain of ideals $A^{[i]}$ of a brace A were defined in [18]. Define $A^{[1]} = A$ and $A^{[i+1]} = \sum_{j=1}^{i} A^{[j]} * A^{[i+1-j]}$. A left brace A is *strongly nilpotent* if there is a number n such that $A^{[n]} = 0$, where $A^{[i]}$ consists of sums of elements $a * b$ with $a \in A^{[j]}, b \in A^{[i-j]}$ for all $0 < j < i$.

All braces and $\mathbb{F}_p$-braces considered in this paper are left braces.

3. Groups and braces

In Example 2 in [16], Rump gave an example of a right brace which is right but not left nilpotent. By taking the opposite multiplication in this brace, we obtain a left brace of cardinality 2^4 which is left but not right nilpotent. Moreover, this brace is an $\mathbb{F}_2$-brace as it is a vector space over $\mathbb{F}_2$. In this section, we show that for a prime number $p > 3$, multiplicative groups of left $\mathbb{F}_p$-braces of cardinality p^4 which are not right nilpotent are isomorphic to either group XIV or group XV described below.

We first recall a result of David Bachiller from [3].

Theorem 3.1 (Lemma 2.5.1, [3]). *Let p be a prime number, and let $(B, +, \circ)$ be a finite left brace with $(B, +)$ isomorphic to C_p^m. Assume $m + 1 \leq p$. Then, the order of each non-trivial element in the multiplicative group $(B, \circ)$ is equal p.*

Therefore, every element in the multiplicative group of any $\mathbb{F}_p$-brace of cardinality p^4 for $p > 3$ has order p. In [4], Burnside described all groups of cardinality p^4 for prime $p > 3$.

Notice that if a brace A of cardinality p^4 has an abelian multiplicative group $(A, \circ)$ then it is a ring, and hence it is both left and right nilpotent [6]. Therefore, a left nilpotent $\mathbb{F}_p$-brace which is left but not right nilpotent has a non-abelian multiplicative group. Therefore, using the list from pages 100, 101 from [4], we have the following possibilities of non-abelian groups of cardinality p^4 in which each element has order p.

- (Group XIV) Group (with multiplication $\circ$) generated by elements P, Q, R, S which is the direct product of the group generated by Q and the group generated by elements P, R, S. Moreover, $P \circ R = R \circ P$, $P \circ S = S \circ P$, $Q \circ P = P \circ Q$ and $R \circ S = S \circ R \circ P$.
- (Group XV) Group (with multiplication $\circ$) generated by elements P, Q, R, S with P being in the centre of this group, and the centre of this group consists of elements P^i. Moreover, $R \circ Q = Q \circ R$ and $Q \circ S = S \circ Q \circ P$ and $R \circ S = S \circ R \circ Q$.

Observe that group XIV has centre of cardinality p^2 and group XV has centre of cardinality p, where by centre we mean the set of elements which commute under operation $\circ$ with all elements in A.

We shall let p be a prime number larger than 3. The aim of this paper is to characterise all not right nilpotent $\mathbb{F}_p$-braces of cardinality p^4. We describe our method for groups of cardinality p^n for any n, as we hope that our approach could be perhaps applied in some other situations.

- Let G be a group of order p^n and $g_1, g_2, \dots, g_n$ be its generators. Let $f_1, f_2, \dots, f_n$ be the defining relations of our group G.
- We will characterise $\mathbb{F}_p$-braces A for which $A = \mathbb{F}_p g_1 + \mathbb{F}_p g_2 + \dots + \mathbb{F}_n g_n$.
- We write $g_i * g_j = \sum_{0<k\leq n} \alpha_{i,j,k} g_k$ where $\alpha_{i,j,k} \in \mathbb{F}_p$ are unknown. As usual $a * b = a \circ b - a - b$ in our brace.
- We substitute these equations in the relations $f_1, f_2, \dots, f_n$ as well as in the relations $f_i * g_j$ for $i, j \leq n$ and find $\alpha_{i,j,k}$ such that the above equations hold. This gives necessary conditions for our brace to be well-defined.
- To check if the brace is well-defined, we proceed as follows: We consider the linear space $B = \mathbb{F}_p g_1' + \dots \mathbb{F}_p g_n'$ for some elements $g_1', g_2', \dots, g_n'$ from some set X. We define maps
$$\lambda_{g_i}(g_j') = g_j' + \sum_{0<k\leq n} \alpha_{i,j,k} g_k'.$$
- Next, we define maps λ_g for $g \in G$ inductively by using the formula $\lambda_{g\circ h}(b) = \lambda_g(\lambda_h(b))$ for $b \in B$. To construct a well defined brace, we then use Theorem 2.1 from [8] with the cocycle $f(g) = \lambda_g(1) - 1$. Notice that, to be able to apply Theorem 2.1, we need to show that $f : G \to B$ is a bijective cocycle. In our case it is done in section 5.3.
- In this way, we can construct all $\mathbb{F}_p$-braces with multiplicative group G and generators $g_1', g_2', \dots, g_n'$ and such that $G = \mathbb{F}_p g_1' + \dots + \mathbb{F}_p g_n'$ (see Section 6 for a method).
- For braces with multiplicative group XV, we can show that we can assume that $A = \mathbb{F}_p g_1 + \dots + \mathbb{F}_p g_n$, provided that the brace is not right nilpotent. This then implies that we constructed all not right nilpotent braces with the multiplicative group G.
- We also show that all $\mathbb{F}_p$-braces with multiplicative group XIV are right nilpotent, and hence strongly nilpotent. Braces of cardinality p^4 for $p = 2, 3$ can be calculated using the GAP package.

4. Braces whose multiplicative group is XV

Let $(G, \circ)$ be the group XV, so the free group generated by elements P, Q, R, S subject to relations

$$Q\circ S = S\circ Q\circ P,$$
$$Q\circ R = R\circ Q,$$
$$P\circ S = S\circ P, P\circ Q = Q\circ P, P\circ R = R\circ P,$$
$$R\circ S = S\circ R\circ Q.$$
$$P^p = Q^p = R^p = S^p = 1_G.$$

Let $(A, +, \circ)$ be a brace whose multiplicative group is G. As usual we have $g \circ h = g * h + g + h$.

We assume that A is not right nilpotent. We recall a result of Rump [16].

Theorem 4.1 ([16]). *If A is a brace of a cardinality p^n for some prime number p and some natural n, then $A^{n+1} = 0$ where $A^1 = A$ and $A^{i+1} = A * A^i$.*

We get the following Corollary.

Corollary 4.2. *Let A be a brace of cardinality p^4. If $A^4 \neq 0$, then A^i/A^{i+1} has cardinality p for $i = 1, ..., 4$.*

Proof. Notice that if A^i/A^{i+1} has cardinality smaller than p, then $A^i = A^{i+1}$, since A^i is an abelian group under the operation $+$. Suppose that $A^i = A^{i+1}$ for some i. Then $A^i = A^{i+1} = A * A^{i+1}$ for some $i < 4$. Then $A^i = A * A^i = A * A^{i+1} = A^{i+2}$. Continuing in this way we get that $A^i = A^4 = A^5 = 0$, which is a contradiction, since we assumed that $A^n \neq 0$. Now we find a chain of subgroups of index at least p given by $A^4 \subset A^3 \subset A^2 \subset A$ which implies that A^i/A^{i+1} has cardinality p since the size of A is p^4. □

Notation 4.3. *Let $(A, +, \circ)$ be a brace. For an element $a \in A$ we will denote by a^{-1} an element in A such that $a \circ a^{-1} = 1 = 0$. Similarly, by a^n, sometimes written at $a^{n\circ}$, we will denote the product of n elements a under the operation $\circ$.*

Note that in any brace the identity element 0 of the additive group $(A, +)$ coincides with the identity element 1 of the multiplicative group $(A, \circ)$.

4.1. Some supporting lemmas. Recall that the λ map in a brace $(A, +, \circ)$ is defined for $a, b \in A$ by

$$\lambda_a(b) = a * b + b = a \circ b - a.$$

It is known that

$$\lambda_{a\circ b}(c) = \lambda_a(\lambda_b(c)).$$

Lemma 4.4. *Let A be an $\mathbb{F}_p$-brace of cardinality p^4. Then for $a, b, c \in A$ we have*

$$\begin{aligned}\left(a^{-1} \circ b^{-1} \circ a \circ b\right) * c = {} & a * (b * c) - b * (a * c) \\ & + a * (b * (a * c)) + b * (b * (a * c)) \\ & - b * (a * (b * c)) - a * (a * (b * c)).\end{aligned}$$

Proof. Note we have $A^5 = 0$. Now using properties of λ and the formula

$$\lambda_a^{-1}(b) = b - a * b + a * (a * b) - a * (a * (a * b)) \text{ for } a, b \in A$$

the result follows by computation. □

Recall that in group XV we have the relation

$$Q = R^{-1} \circ S^{-1} \circ R \circ S.$$

Now, Lemma 4.4 implies the following.

Corollary 4.5. *Let $p > 3$ be a prime. Let $(A, +, \circ)$ be a brace whose multiplicative group is the group XV. Then*

$$Q * A^i \subseteq A^{i+2},\ Q \in A^2.$$

Moreover,

$$Q * Q \in Q * A^2 \subseteq A^4.$$

Furthermore, using the relation in group XV

$$P = Q^{-1} \circ S^{-1} \circ Q \circ S,$$

Lemma 4.4, and Corollary 4.5 we have the following corollary.

Corollary 4.6. *Let $(A, +, \circ)$ be a brace whose multiplicative group is the group XV. Then*

$$P * A^i \subseteq A^{i+3},\ P \in A^3.$$

Therefore,

$$P * P = 0,\ Q * P = 0,\ P * Q = 0,\ A * P = P * A \subseteq A^4,\ P * A^2 = A^2 * P = 0.$$

Proposition 4.7. *Let $p > 3$ be a prime. Let $(A, +, \circ)$ be a brace which is not right nilpotent with multiplicative group XV. Then $A^4 \neq 0$ and*

$$P \notin A^4.$$

Moreover, A^2 is a brace of cardinality p^3 and A^3 is a brace of cardinality p^2, so

$$A^3 = \mathbb{F}_p P + A^4.$$

Proof. Observe first that $P * a = a * P$ for any $a \in A$ since P is central in $(A, \circ)$. Recall $P \in A^3$, so $P * A = A * P \subseteq A^4$. Therefore, $A^4 = 0$ implies that $I = \mathbb{F}_p P$ is an ideal in A and $I * A = A * I = 0$. Notice that A/I has cardinality p^3, and it is known that this implies that A/I is right nilpotent [3]. Now $A * I = I * A = 0$ implies that A is right nilpotent. This contradicts the assumption that A is not right nilpotent.

We will now show that $P \notin A^4$. If $P \in A^4$, then $A * P \subseteq A^5 = 0$, and since P is central, we have $P * A = 0$. Therefore, reasoning similarly to above, $I = \mathbb{F}_p P$ is an ideal in A and A/I is right nilpotent. Therefore, $P \notin A^4$.

Notice that, by Corollary 4.2, $A^4 \neq 0$ implies A^i/A^{i+1} is one dimensional vector space for $i = 1, 2, 3, 4$. It follows that A^2 is a brace of cardinality p^3 and A^3 has cardinality p^2, so $A^3 = \mathbb{F}_p P + A^4$. □

Proposition 4.8. *Let $p > 3$ be a prime. Let $(A, +, \circ)$ be a brace which is not right nilpotent with multiplicative group XV and let $a \in A^4$. Then*

$$a * Q = P^\alpha,$$

for some $1 \leq \alpha \leq p$.

Proof. Consider the element $e = a^{-1}\circ Q^{-1}\circ a\circ Q$ where the inverses are taken in the group $(A,\circ)$. Notice that since $Q * A^i \subseteq A^{i+2}$ and by Lemma 4.4 we get

$$e \in A^3,\ e * A^i \subseteq A^{i+3}.$$

For $r \in A$ denote

$$E_r = e^{-1}\circ r^{-1}\circ e\circ r.$$

Now using similar reasoning as before we get

$$E_r \in A^4,\ E_r * A \subseteq A^5 = 0.$$

Since $E_r \in A^4$, then $A * E_r = 0$. This implies that $\mathbb{F}_p E_r$ is an ideal in A. Therefore, if $E_r \neq 0$, then $A/\mathbb{F}_p E_r$ is a brace of cardinality p^3 or less, and hence it is right nilpotent by [3]. This implies that A is right nilpotent. Since we only consider not right nilpotent braces, this is impossible. Therefore, $E_r = 0$. This holds for every $r \in R$, so it follows that e is in the centre of group $(A,\circ)$. Because the group $(A,\circ)$ is group XV, it follows that $e = P^i$ for some natural number i. Therefore, by writing e as sums of products of Q and a and using the fact that $A * a = 0$ since $a \in A^4$ we get $a * Q = P^\alpha$, for some $0 \leq \alpha < p$ (since $A^3 * A^3 = A^3 * (\mathbb{F}_p P + A^4) = P * A^3 = 0$). □

Proposition 4.9. *Let $p > 3$ be a prime. Let $(A,+,\circ)$ be an $\mathbb{F}_p$-brace which is not right nilpotent with multiplicative group XV. Suppose that $R \notin A^2$ and $Q \notin A^3$. Then there exist element $\bar{S} \in A^4$ such that the mapping $f : (A,\circ) \to (A,\circ)$ given by $f(P) = P$, $f(Q) = Q$, $f(R) = R$, $f(S) = \bar{S}$ is an automorphism of the group $(A,\circ)$.*

Proof. Observe that the mapping $f : G \longrightarrow G$ of the group $G = (A,\circ)$ defined on generators of G by

$$f(R) = R,\ f(Q) = Q,\ f(P) = P,\ f(S) = S\circ R^i\circ Q^j\circ P^k$$

is a group homomorphism for any i, j, k.

Observe that since $R \notin A^2$, then for some i the element $S_2 := S\circ R^i$ will belong to A^2 (because by Corollary 4.6 we have that A/A^2 has dimension 1 as an $\mathbb{F}_p$-vector space). Notice also that since $Q \notin A^3$, then for some j element $S_3 := S_2\circ Q^j$ will belong to A^3.

We know that $P \in A^3$ and $P \notin A^4$. Consequently, for some k we have that element $S_4 = S_3\circ P^k$ will be in A^4. Therefore, $S\circ R^i\circ Q^j\circ P^k \in A^4$. We can now define $\bar{S} = S\circ R^i\circ Q^j\circ P^k$.

It remains to show that f is an automorphism, so the kernel of f is trivial. This follows because the image of a non-trivial element $P^\alpha\circ Q^\beta\circ R^\gamma\circ S^\xi$ will be a non-trivial element (alternatively, it is easy to give the formula for the inverse map f^{-1}). □

4.2. The case when $R \in A^2$.

Lemma 4.10. *Let $p > 3$ be a prime. Let $(A,+,\circ)$ be an $\mathbb{F}_p$-brace whose multiplicative group is the group XV. If $R \in A^2$, then A^2 is a commutative brace.*

Proof. Suppose that $R \in A^2$ so $P, Q, R \subseteq A^2$. Since the set $\{P^i \circ Q^j \circ R^t : 0 < i, j, t \leq p\}$ has cardinality p^3 and is contained in A^2 it follows that $A^2 = \{P^i \circ Q^j \circ R^t : 0 < i, j, t \leq p\}$, by Proposition 4.7. Therefore, $(A^2, \circ)$ is commutative (since P, Q, R commute with each other). It follows that $(A, +, *)$ is a commutative ring by [6]. □

Lemma 4.11. *Let $(A, +, \circ)$ be a brace which is not right nilpotent with multiplicative group XV. If $R \in A^2$, then $Q * Q = 0$.*

Proof. Notice that from the relation

$$R \circ S = S \circ R \circ Q$$

we get

$$R * S = S * R + S * Q + R * Q + Q.$$

therefore,

$$Q * (R * S) = Q * (S * R) + Q * (S * Q) + Q * (R * Q) + Q * Q$$

$$Q * (R * S) = Q * (S * R) + Q * Q \in A^4 \text{ since } Q \in A^2. \tag{2}$$

We have also the group relation $Q \circ R = R \circ Q$, therefore

$$(Q \circ R) * S = (R \circ Q) * S,$$

which implies that $Q * (R * S) = R * (Q * S)$. Now

$$Q * S \in A^3 = \mathbb{F}_p P + A^4,$$

so $R * (Q * S) \in \mathbb{F}_p P * R = 0$. Thus substituting in (2) we find

$$0 = R * (Q * S) = Q * (R * S) = Q * (S * R) + Q * Q,$$

since we have assumed $R \in A^2$, we have that $Q * (S * R) = 0$, so $Q * Q = 0$. □

Proposition 4.12. *Let $(A, +, \circ)$ be an $\mathbb{F}_p$-brace which is not right nilpotent with multiplicative group XV. If $R \in A^2$, then $Q \in A^3$.*

Proof. Suppose on the contrary that $Q \notin A^3$. Recall that, by Corollaries 4.5 and 4.6 and Proposition 4.7, $Q \in A^2$, $P \in A^3$, $P \notin A^4$. Hence,

$$A^2 = \mathbb{F}_p Q + \mathbb{F}_p P + A^4.$$

In group XV we have the relation

$$Q \circ S = S \circ Q \circ P,$$

hence $Q * S = S * Q + S * P + P$, by Corollary 4.6. We also have the relation $R \circ S = S \circ R \circ Q$, so

$$R * S = S * R + S * Q + R * Q + Q$$

(notice that $S * (R * Q) = S * (Q * R) \in S * A^4 \subseteq A^5 = 0$). Also, we have the relation

$$(R \circ S) * S = (S \circ R \circ Q) * S,$$

hence,

$$R * (S * S) = S * (R * S) + S * (Q * S) + Q * S.$$

Observe that $R * (S * S) \subseteq A^2 * A^2$. Recall that A^2 is a commutative ring by Lemma 4.10 and $A^2 = \mathbb{F}_p Q + \mathbb{F}_p P + A^4$, hence

$$A^2 * A^2 = A^2 * (\mathbb{F}_p Q + \mathbb{F}_p P + A^4) \subseteq \mathbb{F}_p Q * Q + \mathbb{F}_p A^2 * P + A^2 * A^4 = 0$$

(since $Q * Q = 0$ by Lemma 4.11 and A^2 is commutative). Next, by the above we have

$$S * (R * S) = S * (S * R + S * Q + R * Q + Q).$$

Therefore,

$$S * Q + Q * S = -(S * (S * R) + S * (S * Q) + S * (Q * S)) \subseteq A^4.$$

Recall from the beginning of this proof that $Q * S - S * Q = S * P + P$, so

$$S * Q \in \frac{-P}{2} + A^4.$$

Therefore, $Q * S \in \frac{P}{2} + A^4$.

Recall the relation

$$(Q \circ S) * S = (S \circ Q \circ P) * S.$$

Hence, $Q * (S * S) = S * (Q * S) + P * S$, and by the above

$$Q * (S * S) \subseteq Q * A^2 \subseteq A^2 * A^2 = 0,$$

and $S * (Q * S) \in S * (\frac{P}{2} + A^4) = \frac{S*P}{2}$. Therefore, $\frac{3}{2} S * P = 0$. Hence $P * A = A * P = 0$ so $\mathbb{F}_p P$ is an ideal in A. Consequently, $A/\mathbb{F}_p P$ is right nilpotent, so A is right nilpotent, a contradiction. □

4.3. The case when $Q \in A^3$.

Theorem 4.13. *Let $p > 3$ be a prime number. Let A be an $\mathbb{F}_p$-brace whose multiplicative group $(A, \circ)$ is the group XV. Suppose that $Q \in A^3$. Then A is a right nilpotent brace.*

Proof. Notice that the set of all products $P^i \circ Q^j$ has cardinality p^2, and we know from Proposition 4.7 that $A^3 = A * (A * A)$ has cardinality p^2. Moreover, $P^i \circ Q^j \in A^3$ (where $P^j = P \circ \cdots \circ P$, where P appears j times in this product). So $A^3 = \{P^i \circ Q^j : i, j \leq p\}$. Since $A^4 \subseteq A^3$, it follows that there are integers i, j and $0 \neq E \in A^4$ such that

$$E = P^i \circ Q^j.$$

We will now consider two cases.

Case 1. Either $S \in A^2$ or both $S, R \notin A^2$. Because A/A^2 has dimension 1. Then there is $0 < j \leq p$ such that

$$S \circ R^j \in A^2.$$

Denote $Z = S \circ R^j$.

By the group relations, we have

$$Q \circ Z = Z \circ Q \circ P.$$

Recall that $Q * P = 0$, so

$$Q * Z = Z * Q + Z * P + P.$$

Notice $Q * Z \in Q * A^2 \subseteq A^4$ and $Z * Q \subseteq Z * A^3 \subseteq A^4$, $Z * P \subseteq Z * A^3 \subseteq A^4$, so

$$P \in A^4.$$

But $P \in A^4$ implies that A is nilpotent, as shown previously.

Case 2. Suppose $S \in A, S \notin A^2$ and $R \in A^2$.

Observe that the group relation

$$Q \circ S = S \circ Q \circ P$$

implies

$$Q * S = S * Q + S * P + P,$$

since $Q * P = 0$ by Corollary 4.6. Therefore,

$$S * (Q * S) = S * (S * Q) + S * (S * P) + S * P = S * P$$

since

$$S * (S * Q) \subseteq S * (S * A^3) \subseteq A^5 = 0.$$

Observe now that we also have a relation

$$(Q \circ S) * S = (S \circ Q \circ P) * S,$$

which implies $Q * (S * S) = S * (Q * S) + P * S$. By the above, $Q * (S * S) = S * (Q * S) + P * S = 2S * P$ (since $P * S = S * P$). Notice that if $S * P = 0$ then $P * A = A * P = 0$ and similarly as in previous section it implies that A is right nilpotent. If $S * P \neq 0$, then $Q * (S * S) \neq 0$. Notice that $A^2 = \mathbb{F}_p R + \mathbb{F}_p Q + \mathbb{F}_p P + A^4$. Therefore,

$$Q * (S * S) \subseteq Q * A^2 = \mathbb{F}_p Q * R + \mathbb{F}_p Q * Q + \mathbb{F}_p Q * P = \mathbb{F}_p Q * R,$$

since $Q \in A^3$. It follows that $Q * R \neq 0$.

Note that because $R \circ Q = Q \circ R$ we get $Q * R = R * Q \neq 0$. Observe that by the above there are i, j such that $Q^i \circ P^j = E \in A^4$, where i is a natural number not divisible by p, since $P \notin A^4$, as $P \in A^4$ would imply that A is a right nilpotent brace (for example by the first Lemma in Section 8). Observe that it follows that $E * R = (Q^i \circ P^j) * R = i(Q * R) \neq 0$ (since $P * R \subseteq P * A^2 = 0$). On the other hand, since $R, P, Q \in A^2$ and A^2 has cardinality p^3 then A^2 is commutative. Therefore, $E * A^2 = A^2 * E \subseteq A^2 * A^4 \subseteq A^5 = 0$, which is a contradiction. Notice that $R \in A^2$ so $E * A^2 = 0$ gives $E * R = 0$. However, we have shown that $E * R$ is not zero above. This gives a contradiction. □

4.4. The case when $S \in A^4$.

Proposition 4.14. *Let $p > 3$ be a prime number. Let A be an $\mathbb{F}_p$-brace whose multiplicative group $(A, \circ)$ is the group XV. Then $(A, \circ)$ is generated by elements P, Q, R, S which satisfy relations from group XV. Moreover, the following relations hold for $a \in \{P, Q, R, S\}$.*

(1)
$$Q \circ S = S \circ Q \circ P,\ (Q \circ S) * a = (S \circ Q \circ P) * a$$
(2)
$$Q \circ R = R \circ Q,\ (Q \circ R) * a = (R \circ Q) * a$$
(3)
$$P \circ S = S \circ P,\ P \circ Q = Q \circ P,\ P \circ R = R \circ P,$$
$$(P \circ S) * a = (S \circ P) * a = 0,\ (P \circ Q) * a = (Q \circ P) * a = 0,\ (P \circ R) * a = (R \circ P) * a$$
(4)
$$R \circ S = S \circ R \circ Q,\ (R \circ S) * a = (S \circ R \circ Q) * a$$
(5)
$$P^p = Q^p = R^p = S^p = 0,\ (P^p) * a = (Q^p) * a = (R^p) * a = (S^p) * a = 0$$

Proof. It follows from the fact that group XV is the multiplicative group $(A, \circ)$ of our brace. Recall that 0 is the identity element of the additive group $(A, +)$ and also the identity element of the multiplicative group $(A, \circ)$ (these identity elements coincide in every brace). □

Proposition 4.15. *Let $p > 3$ be a prime number. Let $(A, +, \circ)$ be an $\mathbb{F}_p$-brace which is not right nilpotent with multiplicative group XV. Then $(A, \circ)$ is generated by elements P, Q, R, S which satisfy relations from group XV. In addition, we have the following.*

(1) $S \in A^4, P \in A^3, P \notin A^4, Q \in A^2$. *Moreover,* $Q * A^i \subseteq A^{i+2}$, $P * A^i \subseteq A^{i+3}$.
(2) $Q \notin A^3, R \in A, R \notin A^2$.
(3) $Q * P = 0, P * P = 0, S * P = 0, R * P = yS$ *for some* $y \in \mathbb{F}_p$ *with* $y \neq 0$.
(4) $Q * S = 0, P * S = 0, S * S = 0, R * S = 0$.
(5) $Q * Q = \alpha S, P * Q = 0, S * Q = \gamma P, R * Q = z_1 P + zS$ *for some* $\alpha, \gamma, z, z_1 \in \mathbb{F}_p$.
(6) $Q * R = z_1 P + zS, P * R = yS$ *for some* $z, z_1, y \in \mathbb{F}_p$ *with* $y \neq 0$.
(7) $S * R = j'Q + i'P + k'S, R * R = jQ + iP + kS$ *for some* $j, j', i, i', k, k' \in \mathbb{F}_p$.
(8) $\gamma = -1$.
(9) $\alpha = -y$.
(10) $j' = -1$.
(11) $z_1 = 0$ *and* $j = 0$.
(12) $2z = y, i' = 1, k' = -z$.

Proof. (1) It follows from Corollary 4.5, Proposition 4.7, Proposition 4.9.

(2) It follows from Proposition 4.12 and Theorem 4.13.
(3) It follows from Corollary 4.5 that $Q * P, P * P, S * P \in A^5 = 0$ (since $S * P = P * S$ as $S \circ P = P \circ S$). Moreover, $R * P \in A^4 = \mathbb{F}_p S$, which gives the conclusion.
(4) It follows from the fact that $S \in A^4$ so $A * S = 0$.
(5) By Corollary 4.5, we have that $P * Q \in A^5 = 0$, $Q * Q \in A^4 = \mathbb{F}_p S$. Similarly, since $Q \in A^2$, then $R * Q \in A^3 = \mathbb{F}_p P + \mathbb{F}_p S$, by item 1 above. The fact that $S * Q = \gamma P$ follows from Proposition 4.8.
(6) Since P is central in the group XV it follows that $P * R = R * P = yS$ by item 3 above. Similarly, $Q * R = R * Q$ since $Q \circ R = R \circ Q$, and the result follows from item 5 above.
(7) Notice that $S * R, R * R \in A^2 = \mathbb{F}_p Q + \mathbb{F}_p P + \mathbb{F}_p S$ by item 1.
(8) Consider the relation

$$S \circ Q \circ P = Q \circ S.$$

It can be rewritten as $S * Q + P + S * P = Q * S = 0$ since $Q * S \subseteq A * A^4 \subseteq A^5 = 0$. This gives $\gamma = -1$.
(9) Consider the relation

$$(R \circ S) * Q = (S \circ R \circ Q) * Q.$$

We get $Q * Q + S * (R * Q) = R * (S * Q)$, hence $\alpha = -y$.
(10) Consider the relation $(S \circ Q \circ P) * R = (Q \circ S) * R$ which is an implication of one of the group relations in group XV. We can rewrite it as

$$S * (Q * R) + P * R = Q * (S * R).$$

This implies $-y = -\alpha j'$. We know that $y \neq 0$ since A is not right nilpotent, and $\alpha = -y$, hence $j' = -1$.
(11) We will first show that $j = -z_1$. Consider the group relation $Q \circ R = R \circ Q$, it implies $(Q \circ R) * R = (R \circ Q) * R$. This implies $Q * (R * R) = R * (Q * R)$, hence $j\alpha = z_1 y$. Since $y \neq 0$ and $y = -\alpha$ we get $z_1 = -j$.

We will now to show that $z_1 = 0$. Consider the relation $(S \circ R \circ Q) * R = (R \circ S) * R$. This implies $S * (R * R) + Q * R + R * (Q * R) = R * (S * R)$ since $S * (Q * R) \subseteq A^5 = 0$. We can consider the component corresponding to P in this equation. This implies $-j + z_1 = j' z_1$, and since $j' = -1$ we get $j = 2z_1$. Since we previously showed that $z_1 = -j$ it follows that $z_1 = j = 0$.
(12) Consider the equation $S * (R * R) + Q * R + R * (Q * R) = R * (S * R)$ from the previous sub-point. Comparing the component at S in this equation we get $z = zj' + i'y$, hence $2z = i'y$.

We will now show that $i' = 1$ hence $2z = y$. We will now consider the relation

$$S \circ R \circ Q = R \circ S.$$

This implies

$$S * R + S * Q + R * Q + Q = 0$$

since $S * (R * Q) \subseteq S * A^3 = 0$ and $R * S \subseteq A * A^4 = A^5 = 0$. Comparing the component at P in this equation we get $i' - 1 = 0$, hence $i' = 1$, as required. Comparing component at S we get $k' + z = 0$ hence $k' = -z$.

□

Remark 4.16. *A general comment on Proposition 4.15 to explain the approach. In first subpoint we show that*

$$A = \mathbb{F}_p P + \mathbb{F}_p R + \mathbb{F}_p S + \mathbb{F}_p Q$$

and then so we can write each product, for example $Q * Q$ as $iP + jR + kS + lQ$ for some i, j, k, l in $\mathbb{F}_p$. Next we substitute it to the equations, which need to hold in the brace, listed in Theorem 4.13, and then list the consequences.

5. The braces are well-defined

5.1. The map λ. We now consider how our operation $*$ looks in our brace. In the previous section we showed that if $(A, +, \circ)$ is brace which is not right nilpotent whose group $(A, \circ)$ is the group XV, then

$$P * P = 0,\ P * Q = 0,\ P * R = yS,\ P * S = 0,$$

$$Q * P = 0,\ Q * Q = -yS,\ Q * R = 2^{-1}yS,\ Q * S = 0,$$

$$R * P = yS,\ R * Q = 2^{-1}yS,\ R * R = iP + kS,\ R * S = 0,$$

$$S * P = 0,\ S * Q = -P,\ S * R = -Q + P - 2^{-1}yS,\ S * S = 0.$$

where $y, i, k \in \mathbb{F}_p$ with $y \neq 0$.

Therefore, we get the formulas for the λ maps in A, where $\lambda_a(b) = a * b + b$.

$$\lambda_P(P) = P,\ \lambda_P(Q) = Q,\ \lambda_P(R) = R + yS,\ \lambda_P(S) = S,$$

$$\lambda_Q(P) = P,\ \lambda_Q(Q) = Q - yS,\ \lambda_Q(R) = R + 2^{-1}yS,\ \lambda_Q(S) = S,$$

$$\lambda_R(P) = P + yS,\ \lambda_R(Q) = Q + 2^{-1}yS,\ \lambda_R(R) = R + iP + kS,\ \lambda_R(S) = S,$$

$$\lambda_S(P) = P,\ \lambda_S(Q) = Q - P,\ \lambda_S(R) = R - Q + P - 2^{-1}yS,\ \lambda_S(S) = S.$$

Let $(B', +)$ be the abelian group generated by elements $Q', P', R', S', 1$ where every element has order p, so $pQ' = pQ' = pR' = pS' = p1 = 0$. Therefore,

$$B' = \mathbb{F}_p P' + \mathbb{F}_p Q' + \mathbb{F}_p R' + \mathbb{F}_p S' + \mathbb{F}_p 1,$$

where 1 is some element of B.

Let $(B, +)$ be the subgroup of $(B', +)$ generated by elements P', Q', R', S'. Define the homomorphisms $\lambda_P, \lambda_Q, \lambda_R, \lambda_S$ from $(B', +)$ to $(B', +)$ by using the table for λ maps in B above, and by setting $\lambda_g(1) = g' + 1$ for $g \in \{P, Q, R, S\}$.

So we have the following relations which depend on parameters $i, k, y \in \mathbb{F}_p$ with $y \neq 0$ given below.

$$\lambda_P(P') = P', \lambda_P(Q') = Q', \lambda_P(R') = R' + yS', \lambda_P(S') = S',$$

$$\lambda_P(1) = P' + 1,$$

$$\lambda_Q(P') = P', \lambda_Q(Q') = Q' - yS', \lambda_Q(R') = 2^{-1}yS' + R', \lambda_Q(S') = S',$$
$$\lambda_Q(1) = Q' + 1,$$

$$\lambda_R(P') = P' + yS', \lambda_R(Q') = Q' + 2^{-1}yS', \lambda_R(R') = iP' + kS' + R',$$
$$\lambda_R(S') = S', \lambda_R(1) = R' + 1,$$

$$\lambda_S(P') = P', \lambda_S(Q') = Q' - P', \lambda_S(R') = R' - Q' + P' - 2^{-1}yS',$$
$$\lambda_S(S') = S', \lambda_S(1) = S' + 1.$$

Theorem 5.1. *Let $p > 3$ be a prime number and $i, k, y \in \mathbb{F}_p$ with $y \neq 0$. Let $(B', +)$ and $(B, +)$ be defined as above. Then both $(B', +)$ and $(B, +)$ are linear spaces over the field $\mathbb{F}_p$. Let linear maps $\lambda_g : (B', +) \longrightarrow (B', +)$ for $g \in \{R, Q, P, S\}$ be defined by lines 1-4 above. Then the following relations hold for any $a \in B'$.*

(1)
$$\lambda_Q(\lambda_S(a)) = \lambda_S(\lambda_Q(\lambda_P(a))),$$

(2)
$$\lambda_Q(\lambda_R(a)) = \lambda_R(\lambda_Q(a)),$$

(3)
$$\lambda_P(\lambda_S(a)) = \lambda_S(\lambda_P(a)),\ \lambda_P(\lambda_Q(a)) = \lambda_Q(\lambda_P(a)),\ \lambda_P(\lambda_R(a)) = \lambda_R(\lambda_P(a)),$$

(4)
$$\lambda_R(\lambda_S(a)) = \lambda_S(\lambda_R(\lambda_Q(a))),$$

(5)
$$\lambda_P^p(a) = \lambda_Q^p(a) = \lambda_R^p(a) = \lambda_S^p(a) = a.$$

Therefore, the maps $\lambda_g : (B', +) \longrightarrow (B', +)$ defined inductively using the formula

$$\lambda_{g \circ g'}(a) = \lambda_g(\lambda_{g'}(a))$$

for $g, g' \in (G, \circ)$ and $a \in (B', +)$ are well defined automorphisms of B'. Moreover, maps $\lambda_g : B \longrightarrow B$ with the domain restricted to B are automorphisms of $(B, +)$.

Proof. To check these properties we will present the λ maps in matrix form, and the above properties can be checked by multiplying the matrices M_g. Write the matrices of the linear maps λ_g for $g \in \{R, Q, P, S\}$ in the base $e_1 = 1, e_2 = R', e_3 = Q', e_4 = P', e_5 = S'$ where e_i denotes the vector with all entries zero except of the i-th entry which is 1. Therefore, we have matrices M_i of dimension 5 such that $\lambda_g(e_j) = M_g e_j$ for each $g \in \{R, Q, P, S\}$ where $e_1 = 1, e_2 = R', e_3 = Q', e_4 = P', e_5 = S'$.

We have the matrices

$$M_P = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & y & 0 & 0 & 1 \end{bmatrix} \qquad M_Q = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 2^{-1}y & -y & 0 & 1 \end{bmatrix}$$

$$M_R = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & i & 0 & 1 & 0 \\ 0 & k & 2^{-1}y & y & 1 \end{bmatrix} \qquad M_S = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 1 & 0 \\ 1 & -2^{-1}y & 0 & 0 & 1 \end{bmatrix}$$

observe now that, by direct calculation, we have

$$M_Q M_S = M_S M_Q M_P,\ M_Q M_R = M_R M_Q,$$

$$M_P M_S = M_S M_P,\ M_P M_Q = M_Q M_P,\ M_P M_R = M_R M_P,$$

$$M_R M_S = M_S M_R M_Q,$$

$$M_P^p = M_Q^p = M_R^p = M_S^p = Id,$$

where Id is the identity matrix. This proves the first part of our theorem.

We can now define maps $\lambda_g : (B', +) \longrightarrow (B', +)$ inductively, using the formula

$$\lambda_{g \circ g'}(a) = \lambda_g(\lambda_{g'}(a)),$$

for $g, g' \in (G, \circ)$ and $a \in (B', +)$. Observe that the maps λ_g are group homomorphisms of $(B', +)$ so they are linear maps over the field $\mathbb{F}_p$, so $\lambda_g(a + b) = \lambda_a(b) + \lambda_g(b)$. This is because they are defined as compositions of maps $\lambda_P, \lambda_Q, \lambda_R, \lambda_S$ which are homomorphisms of $(B', +)$, so

$$\lambda_P(a + b) = \lambda_P(a) + \lambda_P(b),\ \lambda_Q(a + b) = \lambda_Q(a) + \lambda_Q(b),$$
$$\lambda_R(a + b) = \lambda_R(a) + \lambda_R(b),\ \lambda_S(a + b) = \lambda_S(a) + \lambda_S(b).$$

Notice that maps $\lambda_P, \lambda_Q, \lambda_R, \lambda_S$ are linear maps and can be represented by matrices, therefore their compositions are also linear maps. Consequently, for any $g, h, j \in G$

$$\lambda_{(g \circ h) \circ j} = \lambda_{g \circ h} \lambda_j = (\lambda_g \lambda_h)\lambda_j = \lambda_g(\lambda_h \lambda_j) = \lambda_{g \circ (h \circ j)}.$$

We will now show that maps λ_g are automorphisms of B'. Notice that the images of maps $\lambda_P, \lambda_Q, \lambda_R, \lambda_S$ are subsets of $(B', +)$, and that the kernels of these maps are zero. Therefore, the maps $\lambda_P, \lambda_Q, \lambda_R, \lambda_S$ with the domain restricted to $(B, +)$ as maps from $(B, +)$ to $(B, +)$ are automorphisms of $(B, +)$. It follows that maps λ_g with the domain restricted to $(B, +)$ for $g \in G$ are also automorphisms of $(B, +)$ because they are compositions of maps $\lambda_P, \lambda_Q, \lambda_R, \lambda_S$. □

5.2. The map f. Let B, B' and maps $\lambda_g : (B', +) \longrightarrow (B', +)$ be defined as in Theorem 5.1 for some $i, k, y \in \mathbb{F}_p$ with $y \neq 0$ and $p > 3$. We will consider $(B, +)$ as a set B. Define the map $f : G \longrightarrow B$ by

$$f(g) = \lambda_g(1) - 1,$$

for $g \in (G, \circ)$.

Theorem 5.2. *Let B, B' and maps $\lambda_g : (B', +) \longrightarrow (B', +)$ be defined as in Theorem 5.1 for some $i, k, y \in \mathbb{F}_p$ with $y \neq 0$ and $p > 3$. Then the map $f : G \longrightarrow B$ defined as*

$$f(g) = \lambda_g(1) - 1$$

for $g \in (G, \circ)$ is a bijective function from G to B.

Proof. We will now show that f is a bijective function. Observe that groups G and $(B, +)$ have the same cardinality, so to show that f is a bijective function it suffices to show that f is injective.

Suppose on the contrary that f is not bijective. Then we would have $f(g) = f(h)$ for some $g, h \in G$. This implies $\lambda_g(1) = \lambda_h(1)$. Let $g' = h^{-1} \circ g$ so $\lambda_{g'}(1) = 1$. Every element of G can be written as a product of elements of some powers of elements P, Q, R, S. Therefore, there are some integers $0 \leq \alpha, \beta, \gamma, \xi < p$ such that

$$g' = R^{\gamma} \circ Q^{\beta} \circ P^{\alpha} \circ S^{\xi}.$$

Notice that it follows from Theorem 5.1 (using the fact that $\lambda_{a \circ b}(c) = \lambda_a \lambda_b(c)$ several times) that $\lambda_{R^{\gamma} \circ Q^{\beta} \circ P^{\alpha} \circ S^{\xi}}(1) - 1 = \gamma R' + C$ where $C \in \mathbb{F}_p Q' + \mathbb{F}_p P' + \mathbb{F}_p S'$, hence

$$\lambda_{g'}(1) - 1 = \gamma R' + C.$$

Notice that $\lambda_{g'}(1) = 1$ implies $\gamma = 0$, so

$$g' = Q^{\beta} \circ P^{\alpha} \circ S^{\xi}.$$

Notice that it follows from Theorem 5.1 (using the fact that $\lambda_{a \circ b}(c) = \lambda_a \lambda_b(c)$ several times) that $\lambda_{Q^{\beta} \circ P^{\alpha} \circ S^{\xi}}(1) - 1 = \beta Q' + D$ where $D \in \mathbb{F}_p P' + \mathbb{F}_p S'$, hence

$$\lambda_{g'}(1) - 1 = \beta Q' + D.$$

Notice that $\lambda_{g'}(1) = 1$ implies $\beta = 0$, so

$$g' = P^{\alpha} \circ S^{\xi}.$$

Observe now that by Theorem 5.1 we get $\lambda_{g'}(1) = \lambda_{P^{\alpha} \circ S^{\xi}}(1) = \alpha P' + \xi S' + 1$. Therefore, $\lambda_{g'}(1) = 1$ implies $\lambda = \xi = 0$, so $g' = g \circ h^{-1}$ is the identity element in G', and so $g = h$ as required. □

5.3. Bijective cocycles and braces.

Definition 5.3. *Let $(G,\circ)$ be a group, $(H,+)$ be an abelian group, $p : G \longrightarrow \mathrm{Aut}(H)$ be an action and $f : G \longrightarrow H$ be such that for $g,h \in G$ we have*

$$f(g\circ h) = f(g) + p_g(f(h)).$$

Then f is a 1-cocycle with respect to p_g.

The following result is known (cf. Jespers, Cedó, Okninski, Rio [8, Theorem 2]).

Theorem 5.4 (Theorem 2, [8])**.** *Let $(G,\circ)$ be a group, $(H,+)$ be an abelian group, p_g be an automorphism of H for each g in G, and $f : G \longrightarrow H$ be a bijective 1-cocycle with respect to p. Define an operation on G for $g,h \in G$ by*

$$g + h = f^{-1}\left(f(g) + f(h)\right).$$

Then $(G,\circ,+)$ is a brace.

Theorem 5.5. *Let $p > 3$ be a prime number. Let $(G,\circ)$ be the group XV, and let automorphisms of $(B,+)$, given by $\lambda_g : (B,+) \longrightarrow (B,+)$, be defined as in Theorem 5.1 for fixed y,i,k. Then the group $(G,\circ)$ with the addition defined as*

$$g + h = f^{-1}\left(f(g) + f(h)\right),$$

where f is defined as in Theorem 5.2, is a brace.

Proof. By Theorem 5.4, it suffices to show that the map f is a bijective cocycle with respect to the map

$$p_g = \lambda_g.$$

By Theorem 5.2, f is a bijective function. To show that f is a cocycle, we need to show that

$$f(g\circ h) = f(g) + p_g(f(h)).$$

By using the formula

$$f(g) = \lambda_g(1) - 1,$$

the left hand side becomes $f(g\circ h) = \lambda_{g\circ h}(1) - 1$ and the right hand side becomes

$$f(g) + p_g(f(h)) = \left(\lambda_g(1) - 1\right) + \lambda_g\left(\lambda_h(1) - 1\right) = \lambda_{g\circ h}(1) - 1$$

since $\lambda_{a\circ b}(1) = \lambda_a(\lambda_b(1))$ by the definition of λ, and $\lambda_g(x+y) = \lambda_g(x) + \lambda_g(y)$ since λ is a automorphism of $(B',+)$ by Theorem 5.1. □

6. All braces

In this section, we show that in Theorem 5.5 we constructed all the $\mathbb{F}_p$-braces which are not right nilpotent with multiplicative group XV.

We will refer to the Multiplicative Table. The following set of rules will be called the Multiplicative Table.

$$P * P = 0,\ P * Q = 0,\ P * R = yS,\ P * S = 0,$$

$$Q * P = 0,\ Q * Q = -yS,\ Q * R = 2^{-1}yS,\ Q * S = 0,$$
$$R * P = yS,\ R * Q = 2^{-1}yS,\ R * R = iP + kS,\ R * S = 0,$$
$$S * P = 0,\ S * Q = -P,\ S * R = -Q + P - 2^{-1}yS,\ S * S = 0.$$

Notice, that using the formulas $\lambda_a(b) = a * b + b$ we can write the Multiplicative Table in the following form.

$$\lambda_P(P) = P,\ \lambda_P(Q) = Q,\ \lambda_P(R) = R + yS,\ \lambda_P(S) = S,$$
$$\lambda_Q(P) = P,\ \lambda_Q(Q) = Q - yS,\ \lambda_Q(R) = R + 2^{-1}yS,\ \lambda_Q(S) = S,$$
$$\lambda_R(P) = P + yS,\ \lambda_R(Q) = Q + 2^{-1}yS,\ \lambda_R(R) = R + iP + kS,\ \lambda_R(S) = S,$$
$$\lambda_S(P) = P,\ \lambda_S(Q) = Q - P,\ \lambda_S(R) = R - Q + P - 2^{-1}yS,\ \lambda_S(S) = S.$$

We can obtain the Multiplicative Table by putting $a * b = \lambda_a(b) - b$.

Theorem 6.1. *Let $p > 3$ be a prime number. Let $(A, +, \circ)$ be the brace constructed in Theorem 5.5 for fixed $i, k, y \in \mathbb{F}_p$ with $y \neq 0$. Then $(A, +, \circ)$ satisfies the Multiplicative Table above for the same i, k, y.*

Proof. Let $f(g) = \lambda_g(1) - 1$ be defined as in Theorem 5.5. Recall that maps $\lambda_g : B' \to B'$ were defined in Theorem 5.1. By Theorem 5.1 functions λ_g satisfy relations from above Theorem 5.1. Each of them is of the form $\lambda_g(h') = \alpha_1 R' + \alpha_2 Q' + \alpha_3 P' + \alpha_4 S'$, for some $g \in \{P, Q, R, S\}$, $h' \in \{P', Q', R', S'\}$ and $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{F}_p$. Let $h \in G$ be such that $\lambda_h(1) - 1 = h'$. Notice, that our relation can be written as

$$\begin{aligned}(\lambda_{g\circ h}(1) - 1) - (\lambda_g(1) - 1) &= \lambda_g(\lambda_h(1) - 1)\\ &= \alpha_1(\lambda_R(1) - 1) + \alpha_2(\lambda_Q(1) - 1) + \alpha_3(\lambda_P(1) - 1) + \alpha_4(\lambda_S(1) - 1).\end{aligned}$$

Since $\lambda_g(1) - 1 = f(g)$, we can write it as

$$f(g\circ h) - f(g) = \alpha_1 f(R) + \alpha_2 f(Q) + \alpha_3 f(P) + \alpha_4 f(S).$$

So we know that function $f : G \longrightarrow B$ used in Theorem 5.5 satisfies the above relation. Because $f : G \longrightarrow B$ is a bijective function, we can apply the map f to both sides of this relation to obtain an equivalent relation

$$f^{-1}(f(g\circ h) - f(g)) = f^{-1}(\alpha_1 f(R) + \alpha_2 f(Q) + \alpha_3 f(P) + \alpha_4 f(S)).$$

Using the formula for addition in brace $(A, +, \circ)$ from Theorem 5.5, we find that the relation

$$g\circ h - g = \alpha_1 R + \alpha_2 Q + \alpha_3 P + \alpha_4 S$$

holds in brace A. In this way, we can obtain all relations from the Multiplicative Table. □

Theorem 6.2. *Let P, Q, R, S be elements of some set $\mathcal{S}$. Let $(A, +, \circ)$ be an $\mathbb{F}_p$-brace such that $A = \mathbb{F}_p R + \mathbb{F}_p Q + \mathbb{F}_p P + \mathbb{F}_p S$ as a linear $\mathbb{F}_p$-space. Suppose that elements P, Q, R, S satisfy the relations from the Multiplicative Table for fixed $i, k, y \in \mathbb{F}_p$ with $y \neq 0$ and $p > 3$. Then the following holds.*

(1) *P, Q, R, S satisfy the defining relations of the group XV. So the following holds.*

$$Q\circ S = S\circ Q\circ P,\ Q\circ R = R\circ Q,\ P\circ S = S\circ P,\ P\circ Q = Q\circ P,\ P\circ R = R\circ P,$$

$$R\circ S = S\circ R\circ Q,\ P^p = Q^p = R^p = S^p = 0.$$

(2) *Every element from $\mathbb{F}_p R + \mathbb{F}_p Q + \mathbb{F}_p P + \mathbb{F}_p S$ can be written in an unique way as $R^\alpha \circ Q^\beta \circ P^\gamma \circ S^\xi$ for some $\alpha, \beta, \gamma, \xi \leq p$.*

(3) *The multiplication of any two elements from $\mathbb{F}_p R + \mathbb{F}_p Q + \mathbb{F}_p P + \mathbb{F}_p S$ is uniquely determined. Therefore, A is uniquely determined by the Multiplicative Table and by elements i, k, y.*

(4) *The group $(A, \circ)$ is generated as a group by elements P, Q, R, S and it satisfies the relations of group XV, and it has p^4 elements, hence it is group XV.*

(5) *The brace $(A, +, \circ)$ is not right nilpotent.*

Proof. (1) It follows from Theorem 5.1, since maps $\lambda_P, \lambda_Q, \lambda_R, \lambda_S$ defined as $\lambda_g(h) = g\circ h - g$ in brace A have an analogous matrix form as maps $\lambda_P, \lambda_Q, \lambda_R, \lambda_S$ from B' to B' in Theorem 5.1. It also follows by a direct calculation.

(2) Let $a = \alpha R + \beta Q + \gamma P + \xi S$ for some $\alpha, \beta, \gamma, \xi \in \mathbb{F}_p$. Notice that $Q, P, S \in A^2$, by the Multiplicative Table. Consider the element $a_1 = R^{p-\alpha}\circ a$. It follows that $a_1 = -\alpha R + a + c$ for $c \in A^2$ (by the formula $(d\circ b) * a = d * a + d * (b * a) + b * a$ applied several times). Notice that since $P, Q, S \in A^2$ it follows that $R \notin A^2$ as otherwise $A = A^2$, hence $A = A^2 = A * A^2 = A^3$, so $A = A^5 = 0$. Consequently, $A^2 = \mathbb{F}_p Q + \mathbb{F}_p P + \mathbb{F}_p S$. Therefore,

$$a_1 = \beta' Q + \gamma' P + \xi' S,$$

for some $\beta', \gamma', \xi' \in \mathbb{F}_p$.

Consider the element $a_2 = Q^{p-\beta'}\circ a_1$. It follows that $a_2 \in -\beta' Q + a_1 + A^3 + A * a_1 \subseteq A^3$ (since $P, S \in A^3$ and $A * A^2 = A^3$). Notice that $P, S \in A^3$, hence $Q \notin A^3$ as otherwise $A^2 = A^3 = A^4 = A^5 = 0$. Therefore, $a_2 = \gamma'' P + \xi'' S$ for some $\gamma'', \xi'' \in \mathbb{F}_p$. By the Multiplicative Table $P * P = P * S = S * P = S * S = 0$, so $a_2 = P^{\gamma''}\circ S^{\xi''}$, and consequently $a = R^\alpha \circ Q^{\beta'} \circ P^{\gamma''} \circ S^{\xi''}$. This concludes the proof.

(3) Let $a, b \in \mathbb{F}_p$. By item 2 above we can write $a = R^\alpha \circ Q^\beta \circ P^\gamma \circ S^\xi$ for some $\alpha, \beta, \gamma, \xi \leq p$. Then

$$a * b + b = \lambda_a(b) = \lambda_{R^\alpha}(\lambda_{Q^\beta}(\lambda_{P^\gamma}(\lambda_{S^\xi}(b)))),$$

and it can be calculated using the Multiplicative Table to give a concrete element from $\mathbb{F}_p R + \mathbb{F}_p Q + \mathbb{F}_p P + \mathbb{F}_p S$. This determines uniquely a brace $(A, +, \circ)$.

(4) Consider the subgroup A' of $(A, \circ)$ generated by elements R, Q, P, S. Then by item 2 above, we have that A' has cardinality p^4, so $A' = (A, \circ)$.

By item 1 above, A' satisfies all the relations of group XV, which concludes the proof (since A' has the same cardinality as group XV).

(5) Observe that by Multiplicative Table we obtain $(S * Q) * (\frac{-1}{y}R) = S$, so A cannot be right nilpotent.

□

Theorem 6.3. *Let $p > 3$ be a prime number. Let $(A, +, \circ)$ an $\mathbb{F}_p$-brace which is not right nilpotent with multiplicative group $(A, \circ)$ being the group XV. Then the $\mathbb{F}_p$-brace A is isomorphic to some brace constructed in Theorem 5.5.*

Proof. Let $(A, +, \circ)$ be an $\mathbb{F}_p$-brace which is not right nilpotent with multiplicative group $(A, \circ)$ being the group XV. Then $(A, +, \circ)$ satisfies the relations from the Multiplicative Table by Proposition 4.15 for some $i, k, y \in \mathbb{F}_p, y \neq 0$.

Let B be the brace constructed in Theorem 5.5 for the same i, k, y. Then B satisfies the same Multiplicative Table as A, by Theorem 6.1. By Theorem 6.2, item 3, braces which satisfy the same Multiplicative Table coincide, so A and B are isomorphic braces. □

7. Some properties of the constructed braces

Recall that a brace is called prime if product of any two non-zero ideals in this brace is non-zero.

Proposition 7.1. *Let $p > 3$ be a prime number. Let A be a brace constructed in Theorem 5.5 for fixed $y, i, k \in \mathbb{F}_p$ with $y \neq 0$. Then A is a prime brace. Moreover, A contains a non-zero strongly nilpotent (i.e., both right and left nilpotent) ideal A^2.*

Proof. A non-zero ideal I in A contains a non-zero element $c = \alpha_1 R + \alpha_2 Q + \alpha_3 P + \alpha_4 S$ for some $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{F}_p$. If $c \notin A^4$, then when multiplying c from the left several times by either R or Q we obtain some non-zero element in A^4, hence I contains $S \in A^4$. Since every ideal containing S contains Q, P we get that $A^2 \subseteq I$ (since $S * Q = -P$, $S * R = -Q + P - 2^{-1}yS$). Notice that $A^2 * A^2 \neq 0$ since $Q * Q \neq 0$, so A is a prime brace, as every product of non-zero ideals in A is non-zero. Moreover, $(A^2 * A^2) * A^2 = A^2 * (A^2 * A^2) = 0$, so A^2 is a strongly nilpotent ideal in A. □

Example 7.2. *Consider a vector space V spanned by the elements P, Q, R, S over the field $\mathbb{F}_p$ with p elements, with multiplication that satisfies*

$$(a + b)c = ac + bc \text{ and } a(b + c) = ab + ac$$

for all a, b, c in V. Furthermore, the following relations hold in V.

$$PS = SS = QS = RS = PP = SP = QP = PQ = RQ = QR = 0,$$

$$RR = jP + kS,\ QQ = -yS,\ RP = yS,\ SQ = -P,\ PR = yS,\ SR = -Q,$$

where j, k, and non-zero y are arbitrary elements from $\mathbb{F}_p$. Now, it is easily checked that this defines a pre-Lie algebra by verifying that

$$(AB)C - A(BC) = (BA)C - B(AC)$$

is satisfied for any $A, B, C \in \{P, Q, R, S\}$. Hence V is an example of a pre-Lie algebra which is left nilpotent and not right nilpotent.

The relations in V were obtained using the formula found in [20] *for obtaining a pre-Lie algebra from a strongly nilpotent $\mathbb{F}_p$-brace to the brace defined in Theorem* 5.5*, and some relations were guessed as to avoid large calculations.*

8. Braces whose multiplicative group is XIV

In this section, we will show that all $\mathbb{F}_p$-braces whose multiplicative group is XIV are right nilpotent and strongly nilpotent provided that p is a prime number larger than 3. Recall that $\mathbb{F}_p$ is the field of cardinality p.

Lemma 8.1. *Let A be an $\mathbb{F}_p$-brace of cardinality p^4, where $p > 3$ is a prime number. Let i be such that $A^{i+1} = 0$ and suppose there is $0 \neq c \in A^i$ such that $c \circ a = a \circ c$ for all $a \in A$. Then A is a right nilpotent brace.*

Proof. Observe that $c * c = 0$ hence $c^j = jc$ for $j = 1, 2, \dots, p$. Denote $\mathbb{F}_p c = \{c^j : j = 1, 2, \dots, p\}$ by I. Then I is an ideal in brace A, and $I * A = A * I = 0$, since $I = \{c^j : j = 1, 2, \dots, p\}$ and c^j is a central element in A for every j (recall that $c^j = c \circ \cdots \circ c$). Notice that A/I has cardinality not exceeding p^3, hence A/I is a right nilpotent brace by [2]. Now $A * I = 0$ yields that A is a right nilpotent brace. □

Lemma 8.2. *Let A be an $\mathbb{F}_p$-brace of cardinality p^4, where $p > 3$ is a prime number. Suppose that the multiplicative group $(A, \circ)$ is the group XIV. Denote by $W = \{P^i \circ Q^j : i, j = 1, 2, \dots, p\}$. Suppose that A is not a right nilpotent brace. Then the following holds.*

1. *$A^3 \neq 0$.*
2. *Suppose that $Q \in A^2$. If $A^4 = 0$ and $A^3 \neq 0$, then the cardinality of A^2 is p^3 and $A^2 = W + A^3$. Moreover $A^3 * A^2 = 0$.*
3. *Suppose that $Q \in A^2$. If $A^5 = 0$ and $A^4 \neq 0$, then the cardinality of A^2 is p^3 and $A^2 = W + A^4$. Moreover, $A^4 * A^2 = 0$.*

Proof. (1) follows from Lemma 8.1, since $P = R^{-1} \circ S^{-1} \circ R \circ S \in A^2$ by Lemma 4.4 and P is a central element in $(A, \circ)$.

(2) Notice that since $Q \in A^2$, then $W \subseteq A^2$. By Lemma 8.1, we have $W \cap A^3 = 0$, since W consists of central elements. Therefore, $W + A^3, A^3 \circ W \subseteq A^2$, and since $A^2 \neq A$ and $W + A^3$ has cardinality p^3, it follows that A^2 has cardinality p^3 and $A^2 = W + A^3 = A^3 \circ W$.

Observe now that

$$A^3 * A^2 = A^3 * (W + A^3) = A^3 * W + A^3 * A^3 = W * A^3 \subseteq A^4 = 0.$$

(3) Notice that since $Q \in A^2$, then $W \subseteq A^2$. By Lemma 8.1, we have $W \cap A^4 = 0$, since W consists of central elements. Therefore, $W + A^4, A^4 \circ W \subseteq A^2$, and since $A^2 \neq A$ and $W + A^4$ has cardinality p^3, it follows that A^2 has cardinality p^3 and $A^2 = W + A^4 = A^4 \circ W$.

Observe now that

$$A^4 * A^2 = A^4 * (W + A^4) = A^4 * W + A^4 * A^4 = W * A^4 \subseteq A^5 = 0.$$

□

Lemma 8.3. *Let A be an $\mathbb{F}_p$-brace of cardinality p^4, where $p > 3$ is a prime number. Suppose that the multiplicative group $(A, \circ)$ is the group XIV. Suppose that A is not a right nilpotent brace. Suppose that $Q \in A^2$ and $R \notin A^2$. Then $P * R = R * P = 0$.*

Proof. Notice that A/A^2 has cardinality p, by Lemma 8.2. Therefore, $S \circ R^i \in A^2$ for some i, since $R \notin A^2$. Let W be as in Lemma 8.2. By Lemma 8.2, we have $S \circ R^i = c \circ w$ for some $w \in W$ and some $c \in A^i$ where $A^{i+1} = 0$. Therefore, $S' = S \circ R^i \circ w^{-1} \in A^i$ (where $A^{i+1} = 0$). Recall that w is a central element, so $R \circ S' = S' \circ R \circ P$. This implies that

$$0 = S' * R + S' * P + S' * (R * P) + R * P + P.$$

Notice that $S' * A^2 = 0$ by Lemma 8.2, so $S' * R + R * P + P = 0$.

Observe now that $(R \circ S') * R = (S' \circ R \circ P) * R$. Therefore, $R * (S' * R) = R * (P * R) + P * R$, since $S' * A^2 = 0$. Substituting $S' * R = -(R * P + P)$ in the left hand side we get $R * (R * P) + R * P = 0$, so $\lambda_R(R * P) = 0$, hence $R * P = 0$, as the map $\lambda_a(b) = a * b + b$ is an invertible map in any brace. □

Lemma 8.4. *Let A be an $\mathbb{F}_p$-brace of cardinality p^4, where $p > 3$ is a prime number. Suppose that the multiplicative group $(A, \circ)$ is the group XIV. Suppose that A is not right nilpotent. Suppose that $Q \in A^2$ and $R \in A^2$. Then $S \notin A^2$ and $P * S = S * P = 0$.*

Proof. Notice that $S \notin A^2$ as otherwise $(A, \circ)$ would be generated by elements from A^2 implying $A = A^2$, which is impossible as then

$$A = A^2 = A * A^2 = A^3 = A^4 = A^5 = 0.$$

Notice that $R \in A^2$ implies that $R = a \circ w$ for some $a \in A^i, w \in W$, where $A^{i+1} = 0$, by Lemma 8.2. Therefore, $R' = R \circ w^{-1} \in A^i$. Notice that since w is central in the group $(A, \circ)$, we get $R' \circ S = S \circ R' \circ P$. Consequently, $R' * S = S * P + P$ since $A * R' = 0$ and $R' * P \subseteq R' * A^2 = 0$ by Lemma 8.2.

Observe now that $(R' \circ S) * S = (S \circ R' \circ P) * S$, hence

$$R' * (S * S) = S * (R' * S) + S * (R' * (P * S)) + S * (P * S) + R' * (P * S) + P * S.$$

Recall that $R' * A^2 = 0$ and $A * R' = 0$ by Lemma 8.2; consequently,

$$0 = S * (R' * S) + P * S + S * (P * S).$$

Substituting $R' * S = S * P + P$ in the right hand side we get

$$0 = S * (S * P + P) + P * S + S * (P * S),$$

therefore $2\lambda_S(S * P) = 0$, so $S * P = 0$. □

Proposition 8.5. *Let A be an $\mathbb{F}_p$-brace of cardinality p^4, where $p > 3$ is a prime number. Suppose that the multiplicative group $(A, \circ)$ is the group XIV. Suppose that A is not a right nilpotent brace. Then $Q \notin A^2$.*

Proof. Suppose on the contrary that $Q \in A^2$. If $R \notin A^2$, then $P * R = 0$ by Lemma 8.3. Observe that $A = \mathbb{F}_p R + A^2$, since A/A^2 has cardinality p, by Lemma 8.2. Observe now that for $x, y \in A$ we have $(P \circ x) * y = (x \circ P) * y$, and by Lemma 4.4 we get

$$\begin{aligned} P * (x * y) &= x * (P * y) \subseteq x * (P * (\mathbb{F}_p R + A^2)) \\ &= x * P * (A^2) \subseteq x * A^4 \subseteq A^5 = 0 \end{aligned}$$

(since $P = R^{-1} \circ S^{-1} \circ R \circ S$ is in group *XIV*). Consequently, $P * A^2 = 0$, and since $P * R = 0$, then $P * A = 0$. Since P is a central element, we get that $I = \mathbb{F}_p P$ is an ideal in A. By [2], every brace of cardinality not exceeding p^3 is right nilpotent, hence A/I is right nilpotent. Now $A * P = 0$ yields that A is right nilpotent.

Suppose now that $R \in A^2$. Then by Lemma 8.4 we have that $S \notin A^2$, $S * P = P * S = 0$. Observe that $A = \mathbb{F}_p S + A^2$, since A/A^2 has cardinality p, by Lemma 8.2. Observe now that for $x, y \in A$ we have $(P \circ x) * y = (x \circ P) * y$, and by Lemma 4.4 we get

$$\begin{aligned} P * (x * y) &= x * (P * y) \subseteq x * (P * (\mathbb{F}_p S + A^2)) \\ &= x * P * (A^2) \subseteq x * A^4 \subseteq A^5 = 0 \end{aligned}$$

(since $P = R^{-1} \circ S^{-1} \circ R \circ S$ is in group XIV). Consequently, $P * A^2 = 0$, and since $P * S = 0$, then $P * A = 0$. Since P is a central element, we get that $I = \mathbb{F}_p P$ is an ideal in A. By [2] every brace of cardinality not exceeding p^2 is right nilpotent, hence $A * R$ is right nilpotent. Now $A * P = 0$ yields that A is right nilpotent. □

Proposition 8.6. *Let A be an $\mathbb{F}_p$-brace of cardinality p^4, where $p > 3$ is a prime number. Suppose that the multiplicative group $(A, \circ)$ is the group XIV. Suppose that $Q \notin A^2$. Then A is a right nilpotent brace.*

Proof. Notice that $P \in A^2$ by Lemma 4.4, since $P = R^{-1} \circ S^{-1} \circ R \circ S$ in the group XIV. By Lemma 8.2 we have that A/A^2 has cardinality p, so $S \circ Q^i \in A^2, R \circ Q^j \in A^2$, for some i, j, since $Q \notin A^2$. We have now the following cases.

Case 1. $P \notin A^3$, $A^4 \neq 0$. Notice that this implies that A^2/A^3 has cardinality p, and so there are k, l such that $S' = S \circ Q^i \circ P^k \in A^3$ and $R' = R \circ Q^j \circ P^l \in A^3$. Notice that since Q, P are central elements we get $P = R'^{-1} \circ S'^{-1} \circ R' \circ S'$, hence by Lemma 4.4 we have $P \in A^4$. By Lemma 8.1 we find that A is right nilpotent.

Case 2. $P \notin A^3$, $A^4 = 0$. Denote by $S' = S \circ Q^i \in A^2, R' = R \circ Q^j \in A^2$. We know that $R', S' \in A^2$. Notice that since Q is central we get $P = R'^{-1} \circ S'^{-1} \circ R' \circ S'$, hence by Lemma 4.4 we have $P \in A^3$. By Lemma 8.1 we find that A is right nilpotent.

Case 3. $P \in A^3$. Notice that $A^4 \neq 0$ and $P \notin A^4$ by Lemma 8.2 since P is central. By Corollary 4.2 we have A^i/A^{i+1} has cardinality p for $i = 1, 2, 3, 4$. Therefore, $A^3 = \mathbb{F}_p P + A^4$ and $A = \mathbb{F}_p Q + A^2$.

Suppose that there are R', S' such that $R' \circ S' = S' \circ R' \circ P$, and either $S' \in A^2, R' \in A^4$ or $S' \in A^4$ and $R' \in A^2$. We will show that $P * Q = 0$.

Suppose first that $S' \in A^4$ and $R' \in A^2$. Observe that

$$(R' \circ S') * Q = (S' \circ R' \circ P) * Q,$$

hence $P * Q = 0$, because $S' * Q = Q * S' \in A^5 = 0$,

$$A * (P * Q) \subseteq A * (Q * P) \subseteq A^5 = 0,$$

$$S' * (R' * Q) = S' * (Q * R') \subseteq S' * A^3 = S' * (\mathbb{F}_p P + A^4) = \mathbb{F}_p (S' * P) = 0,$$

since $S' * P = P * S' \subseteq A^5 = 0$.

Suppose now that $S' \in A^2$ and $R' \in A^4$. Observe that $(R' \circ S') * Q = (S' \circ R' \circ P) * Q$, hence $P * Q = 0$ since $R' * Q = Q * R' \in A^5 = 0$,

$$A * (P * Q) \subseteq A * (Q * P) \subseteq A * A^4 \subseteq A^5 = 0,$$

$$R' * (S' * Q) = R' * (Q * S') \subseteq R' * A^3 = R' * (\mathbb{F}_p P + A^4) = \mathbb{F}_p (R' * P) = 0,$$

since $R' * P = P * R' \subseteq A^5 = 0$.

We will now show that $P * Q = 0$ implies that A is a right nilpotent brace. Observe that $P * A = P * (F_p Q + A^2) = P * A^2$, so we need to show that $P * A^2 = 0$. Notice that $(P \circ x) * y = (x \circ P) * y$ since P is central. Consequently,

$$\begin{aligned} P * (x * y) &= x * (P * y) = x * (P * (\mathbb{F}_p Q + A^2)) \\ &= \mathbb{F}_p x * (P * Q) + x * (P * (A^2)) = 0, \end{aligned}$$

since $P * A^2 \subseteq A^4$ by Corollary 4.6, and $P * Q = Q * P \in A^4$.

We will now show that it is possible to find such R', S'. We know that $R \circ Q^j$ and $S \circ Q^i$ are both in A^2. Suppose that $R \circ Q^j \in A^3$. Then $R \circ Q^j \circ P^k \in A^4$ for some k, and we can take $R' = R \circ Q^j \circ P^k$ and $S' = S \circ Q^i$ (since P, Q are central). If $S \circ Q^i \in A^3$, then $S \circ Q^i \circ P^k \in A^4$ for some k, and we can take $S' = S \circ Q^i \circ P^k$ and $R' = R \circ Q^j$.

If $S \circ Q^i, R \circ Q^j \notin A^3$, then $(S \circ Q^i) \circ (R \circ Q^j)^t \in A^3$ for some t, and then

$$(S \circ Q^i) \circ (R \circ Q^j)^t \circ P^k \in A^4$$

for some k. Therefore, we can take $S' = (S \circ Q^i) \circ (R \circ Q^j)^t \circ P^k$ and $R' = R \circ Q^j$. Observe that $R' \circ S' = S' \circ R' \circ P$, as required. □

Corollary 8.7. *Let A is an $\mathbb{F}_p$-brace for a prime number $p > 3$. If the multiplicative group of A is isomorphic to the group XIV, then A is right nilpotent.*

9. Conclusions and applications

In this section, we give some motivation for constructing concrete example of braces of a given cardinality. Two main applications of braces are set-theoretic solutions and Hopf-Galois extensions. The connection between braces and Hopf-Galois extensions was first observed by David Bachiller in [3]. This topic was subsequently investigated in [21], [12] and many other papers by Truman, Kohl, Byott, Childs and others. The following exposition follows the above literature on the topic.

9.1. Hopf-Galois extensions corresponding to a brace. All Hopf-Galois structures of type $(A,+)$ arise as regular subgroups of $\mathrm{Hol}(A,+)$, cf. [3, 2, 12, 13] for relevant definitions and further details. Now for each brace $(A,+,\circ)$ we have that $(A,\circ)$ embeds in $\mathrm{Hol}(A,+)$ as a regular subgroup through the map

$$m : (A,\circ) \longrightarrow \mathrm{Hol}(A,+), \quad a \longmapsto a\lambda_a.$$

Isomorphic braces correspond to regular subgroups which are conjugate by an element of $\mathrm{Aut}(A,+)$ inside $\mathrm{Hol}(A,+)$. On the other hand, each regular subgroup $G \subset \mathrm{Hol}(A,+)$ gives a bijection

$$\psi : G \longrightarrow (A,+), \quad g \longmapsto g(0),$$

through which we can define a multiplication on $(A,+)$ by

$$a \circ b = \psi\left(\psi^{-1}(a)\psi^{-1}(b)\right)$$

which yields a brace $(A,+,\circ)$.

Therefore, given a brace $(A,+,\circ)$ and an automorphism $\gamma \in \mathrm{Aut}(A,+)$, we can create, another isomorphic brace $(A,+,\circ_\gamma)$ by embedding

$$\begin{array}{ccc} (A,\circ) & \xrightarrow{m} & G \subset \mathrm{Hol}\,(A,+) \\ & & \wr \downarrow C_\gamma \\ & & G_\gamma = \gamma G \gamma^{-1} \end{array} \xrightarrow{\psi} (A,+).$$

The new circle operation is through

$$a \circ_\gamma b = \psi\left(\psi^{-1}(a)\psi^{-1}(b)\right)$$

in terms of holomorph. This corresponds to defining

$$a \circ_\gamma b = \gamma^{-1}\left(\gamma(a) \circ \gamma(b)\right)$$

as in this case $(A,+,\circ)$ and $(A,+,\circ_\gamma)$ are isomorphic as braces, so they correspond to regular subgroups inside holomorph which are conjugate by γ.

Now if $\gamma \in \mathrm{Aut}(A,+,\circ)$, then $(A,+,\circ)$ and $(A,+,\circ_\gamma)$ are the same and that means $G_\gamma = G$ inside the holomorph. For a brace $(A,+,\circ)$ and for each coset representative $\gamma \in \mathrm{Aut}(A,+)/\mathrm{Aut}(A,+,\circ)$, we find a distinct Hopf-Galois structure $(A,+,\circ_\gamma)$. As we move through the braces with additive group $(A,+)$, we get all the Hopf-Galois structures of type $(A,+)$.

Therefore, we can summarise on how to construct Hopf-Galois extensions corresponding to a given brace as follows:

(1) Let $(A, +, \circ)$ be a brace.
(2) Let γ_i be the automorphisms of the abelian group $(A, +)$.
(3) Check which γ_i are also automorphisms of the whole brace $(A, +, \circ)$.
(4) We find coset representatives of $\mathrm{Aut}(A, +)/\mathrm{Aut}(A, +, \circ)$ and call them $\xi_1, \xi_2, \ldots$. Recall that α and β are the same in $\mathrm{Aut}(A, +)/\mathrm{Aut}(A, +, \circ)$ iff $\alpha = \beta\gamma$ for some $\gamma \in \mathrm{Aut}(A, +, \circ)$ (so $\alpha(a) = \beta(\gamma(a))$ for all $a \in A$).
(5) For the automorphisms ξ_i of the group $(A, +)$ from our list above we find the brace $(A_{\xi_i}, +, \circ_{\xi_i})$, with the same set A_{ξ_i} as the set A and with the same addition and with the multiplication
$$a \circ_{\xi_i} b = \xi_i^{-1}(\xi_i(a) \circ \xi_i(b)).$$
(6) For the brace A_{ξ_i} the corresponding Hopf-Galois extension is the regular subgroup (a, λ_a) (denoted above as $a\lambda_a$) of the holomorph $\mathrm{Hol}(A, +)$ where
$$\lambda_a(b) = a \circ_{\xi_i} b - a.$$

Since we now know how to construct Hopf-Galois extensions corresponding to the given brace, we can now obtain all Hopf-Galois extensions of type $(A, +)$ with Galois group G. Following the beginning of this chapter, it can be summarised in the following way.

(1) Find all non-isomorphic braces $(B, +, \circ)$ whose additive group $(B, +)$ is isomorphic to the group $(A, +)$ and whose multiplicative group $(B, \circ)$ is isomorphic to G.
(2) We list these non-isomorphic braces as $B_1, B_2, \ldots$. All these braces have the same additive group, which is isomorphic to $(A, +)$, and the same multiplicative group, which is isomorphic to G.
(3) For each brace B_i from our list we will construct corresponding Hopf-Galois extensions.
(4) To get all Hopf-Galois extensions of type $(A, +)$ with Galois group G we need to collect all the Hopf-Galois extensions constructed for every brace B_i. All these Hopf-Galois extensions are distinct.

The above reasoning can be applied to any brace, so in particular can be applied to all braces constructed in our paper. This would involve some calculations to characterise automorphisms of the constructed braces, so we omitted the calculations and only explained the main ideas in this chapter.

References

[1] Acri, Emiliano; Bonatto Marco. Skew braces of size pq. *Comm. Algebra* **48** (2020), no. 5, 1872–1881. MR4085764, Zbl 1437.16027, arXiv:1908.03228, doi: 10.1080/00927872.2019.1709480. 495

[2] Bachiller, David. Classification of braces of order p^3. *J. Pure Appl. Algebra* **219** (2015), no. 8, 3568–3603. MR3320237, Zbl 1312.81099, arXiv:1407.5224, doi: 10.1016/j.jpaa.2014.12.013. 495, 515, 517, 519

[3] BACHILLER, DAVID. Counterexample to a conjecture about braces. *J. Algebra* **453** (2016), 160–176. MR3465351, Zbl 1338.16022, arXiv:1507.02137, doi: 10.1016/j.jalgebra.2016.01.011. 497, 500, 501, 519

[4] BURNSIDE, WILLIAM. Theory of groups of finite order. EBook, 40395. *Project Gutenberg, Urbana, Illinois*, 2012. xv+456 pp. https://www.gutenberg.org/ebooks/40395. 497

[5] CATINO, FRANCESCO; RIZZO ROBERTO. Regular subgroups of the affine group and radical circle algebras. *Bull. Aust. Math. Soc.* **79** (2009), no. 1, 103–107. MR2486886, Zbl 1184.20001, doi: 10.1017/S0004972708001068. 496

[6] CEDÓ, FERRAN; JESPERS ERIC; OKNIŃSKI, JAN. Braces and the Yang–Baxter equation. *Comm. Math. Phys.* **327** (2014), no. 1, 101–116. MR3177933, Zbl 1287.81062, arXiv:1205.3587, doi: 10.1007/s00220-014-1935-y. 496, 497, 502

[7] CEDÓ, FERRAN; JESPERS ERIC; OKNIŃSKI, JAN. Primitive set-theoretic solutions of the Yang–Baxter equation. *Commun. Contemp. Math.* (2022). arXiv:2003.01983, doi: 10.1142/S0219199721501054.

[8] CEDÓ, FERRAN; JESPERS ERIC; DEL RIO, ÁNGEL. Involutive Yang–Baxter groups. *Trans. Amer. Math. Soc.* **362** (2010), no. 5, 2541- 2558. MR2584610, Zbl 1188.81115, arXiv:0803.4054, doi: 10.1090/S0002-9947-09-04927-7. 498, 511

[9] DIETZEL, CARSTEN. Braces of order p^2q. *J. Algebra. Appl.* **20** (2021), no. 8, Paper No. 2150140. 24 pp. MR4297324, Zbl 07411750, arXiv:1801.06911, doi: 10.1142/S0219498821501401. 495

[10] GATEVA-IVANOVA, TATIANA. Set-theoretic solutions of the Yang–Baxter equation, braces and symmetric groups. *Adv. Math.* **338** (2018), 649–701. MR3861714, Zbl 1437.16028, arXiv:1507.02602, doi: 10.1016/j.aim.2018.09.005. 494

[11] GUARNIERI, LEANDRO; VENDRAMIN, LEANDRO. Skew braces and the Yang–Baxter equation. *Math. Comp.***86**, (2017), no. 307, 2519–2534. MR3647970, Zbl 1371.16037, arXiv:1511.03171, doi: 10.1090/mcom/3161. 495

[12] NEJABATI ZENOUZ, KAYVAN. Skew braces and Hopf–Galois structures of Heisenberg type. *J. Algebra* **524** (2019), 187–225. MR3905210, Zbl 1444.16049, arXiv:1804.01360, doi: 10.1016/j.jalgebra.2019.01.012. 519

[13] NEJABATI ZENOUZ, KAYVAN. On Hopf-Galois Structures and Skew Braces of Order p^3. Ph.D. thesis. The University of Exeter, 2018. 495, 519

[14] RUMP, WOLFGANG. Classification of cyclic braces. *J. Pure. Appl. Algebra* **209** (2007), no. 3, 671–685. MR2298848, Zbl 1170.16031, doi: 10.1016/j.jpaa.2006.07.001. 495

[15] RUMP, WOLFGANG. Classification of cyclic braces. II. *Trans. Amer. Math. Soc.* **372** (2019), no. 1, 305–328. MR3968770, Zbl 1417.81140, doi: 10.1090/TRAN/7569. 495

[16] RUMP, WOLFGANG. Braces, radical rings, and the quantum Yang–Baxter equation. *J. Algebra* **307** (2007), no. 1, 153–170. MR2278047, Zbl 1115.16022, doi: 10.1016/j.jalgebra.2006.03.040. 496, 497, 499

[17] RUMP, WOLFGANG. The brace of a classical group. *Note. Mat.* **34** (2014), no. 1, 115-144. MR3291816, Zbl 1344.14029, doi: 10.1285/I15900932V34N1P115. 495, 496

[18] SMOKTUNOWICZ, AGATA. On Engel groups, nilpotent groups, rings, braces and the Yang–Baxter equation. *Trans. Amer. Math. Soc.* **370** (2018), no. 9, 6535–6564. MR3814340, Zbl 1440.16040, arXiv:1509.00420, doi: 10.1090/tran/7179. 497

[19] SMOKTUNOWICZ, AGATA. Algebraic approach to Rump's results on relations between braces and pre-Lie algebras. *J. Algebra. Appl.* (2020). arXiv:2007.09403, doi: 10.1142/S0219498822500542.

[20] SMOKTUNOWICZ, AGATA. A new formula for Lazard's correspondence for finite braces and pre-Lie algebras. *J. Algebra* **594** (2022), 202–229. MR4353236, Zbl 07459375, arXiv:2011.07611, doi: 10.1016/j.jalgebra.2021.11.027. 495, 515

[21] SMOKTUNOWICZ, AGATA; VENDRAMIN, LEANDRO. On skew braces (with an appendix by N. Byott and L. Vendramin) *J. Comb. Algebra* **2** (2018), no. 1, 47–86. MR3763907, Zbl 1416.16037, arXiv:1705.06958, doi: 10.4171/JCA/2-1-3. 495, 519

[22] VENDRAMIN, LEANDRO. Problems on skew left braces. *Adv. Group Theory Appl.* **7** (2019), 15–37. MR3974481, Zbl 1468.16050, arXiv:1807.06411, doi: 10.32037/agta-2019-003. 495

(D. Puljić) SCHOOL OF MATHEMATICS, THE UNIVERSITY OF EDINBURGH, JAMES CLERK MAXWELL BUILDING, THE KINGS BUILDINGS, MAYFIELD ROAD EH9 3JZ, EDINBURGH, UK
s1557452@sms.ed.ac.uk

(A. Smoktunowicz) SCHOOL OF MATHEMATICS, THE UNIVERSITY OF EDINBURGH, JAMES CLERK MAXWELL BUILDING, THE KINGS BUILDINGS, MAYFIELD ROAD EH9 3JZ, EDINBURGH, UK
A.Smoktunowicz@ed.ac.uk

(K. Nejabati Zenouz) SCHOOL OF COMPUTING AND MATHEMATICAL SCIENCES, THE UNIVERSITY OF GREENWICH, QUEEN MARY'S BUILDING, PARK ROW, SE10 9LS, LONDON, UK
K.NejabatiZenouz@greenwich.ac.uk

This paper is available via http://nyjm.albany.edu/j/2022/28-19.html.